

Scan Vulnerabilities Report

*TENDERO INC (DBA
COGNILLO)*

February 12 2026

PREPARED BY:
SecurityMetrics
1275 W. 1600 N.
Orem, UT 84057

Executive Summary

Scan target: cognillo.com	Maximum Score: 1.00	Start: 2026-01-05 10:43:22
Scan ID: 13248523	Scan Expiration: 2026-04-05	Finish: 2026-01-05 11:24:28
Scan Compliance Status: Passing	TCP/IP Fingerprint PS Estimate: Linux Kernel 2.6	Scan Length: 0:41:06

Introduction

SecurityMetrics has determined that Tendero Inc (DBA Cognillo) is COMPLIANT with the PCI scan validation requirement for this target.
Congratulations, the target **passes** because no failing vulnerability was found.

Port Scan

Attackers use a port scan to find out what programs are running on your system. Most programs have known security weaknesses, so it is best practice to disable any unnecessary programs listed below.

Protocol	Port	Program
TCP	80	Apache httpd
TCP	443	Apache httpd

Scan Results

The following section lists all security vulnerabilities detected on your system. Vulnerabilities which cause you to fail PCI compliance have a score of 4.0 or higher and are listed in red.

Security Vulnerabilities

Protocol	Port	Service	Score	Summary
TCP	443	www	✓ 1.00	Title: TLS ALPN Supported Protocol Enumeration Synopsis: The remote host supports the TLS ALPN extension. Impact: The remote host supports the TLS ALPN extension. This plugin enumerates the protocols the extension supports. See also : https://tools.ietf.org/html/rfc7301 Resolution: n/a Data Received: http/1.1

TCP	None	general	✓ 1.00	Title: OS Fingerprints Detected Synopsis: Multiple OS fingerprints were detected. Impact: Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc), it was possible to gather one or more fingerprints from the remote system. While the highest-confidence result was reported in plugin 11936, "OS Identification", the complete set of fingerprints detected are reported here. Resolution: n/a Data Received: Following OS Fingerprints were found Remote operating system : AXIS P5655-E Confidence level : 56 Method : MLSinFP Type : unknown Fingerprint : unknown Remote operating system : Linux Kernel 2.6 Confidence level : 65 Method : SinFP Type : general-purpose Fingerprint : SinFP: P1:B10113:F0x12:W62727:O0204ffff:M1460: P2:B10113:F0x12:W62643:O0204ffff0402080affffffff4445414401030307:M1460: P3:B00000:F0x00:W0:O0:M0 P4:191500_7_p=80R Following fingerprints could not be used to determine OS : HTTP://Server: Apache SSLcert://i/CN:Sectigo RSA Domain Validation Secure Server CAi/O:Sectigo Limiteds/CN:*.cognillo.com 825a8fdd536e092fdcc59a7c33ec8fe811fc4f3
-----	------	---------	--------	--

TCP	443	www	✓ 1.00	Title: Remote Services Not Using Post-Quantum Ciphers Synopsis: Reports remote services that do not offer post-quantum ciphers. Impact: This plugin reports network services that do not offer post-quantum ciphers. Tenable makes no attempt to determine whether the remote service would be vulnerable to a post-quantum attack. However, cryptography that depends on the classic difficulty of solving the discrete logarithm problem or on the classic difficulty of large prime factorization is broken by Shor's algorithm. Examples of this are RSA asymmetric encryption and Diffie-Hellman key exchange. See also : http://www.nessus.org/u?7a390f87 http://www.nessus.org/u?ad7d6b3b http://www.nessus.org/u?1c0c61e0 http://www.nessus.org/u?5eec4b28 Resolution: n/a Data Received: The target TLS server offers no post-quantum ciphers.
TCP	443	www	✓ 1.00	Title: TLS Version 1.2 Protocol Detection Synopsis: The remote service encrypts traffic using a version of TLS. Impact: The remote service accepts connections encrypted using TLS 1.2. See also : https://tools.ietf.org/html/rfc5246 Resolution: N/A Data Received: TLSv1.2 is enabled and the server supports at least one cipher.

TCP	443	www	✓ 1.00	Title: TLS Version 1.3 Protocol Detection Synopsis: The remote service encrypts traffic using a version of TLS. Impact: The remote service accepts connections encrypted using TLS 1.3. See also : https://tools.ietf.org/html/rfc8446 Resolution: N/A Data Received: TLSv1.3 is enabled and the server supports at least one cipher.
TCP	443	www	✓ 1.00	Title: SSL Cipher Suites Supported Synopsis: The remote service encrypts communications using SSL. Impact: This plugin detects which SSL ciphers are supported by the remote service for encrypting communications. See also : https://www.openssl.org/docs/man1.0.2/man1/ciphers.html http://www.nessus.org/u?e17ffced Resolution: n/a Data Received: Here is the list of SSL ciphers supported by the remote server : Each group is reported per SSL Version. SSL Version : TLSv13 High Strength Ciphers (>= 112-bit key) Name Code KEX Auth Encryption MAC ----- ----- TLS_AES_256_GCM_SHA384 0x13, 0x02 - - AES-GCM(256) SHA384 SSL Version : TLSv12 High Strength Ciphers (>= 112-bit key) Name Code KEX Auth Encryption MAC ----- ECDHE-RSA-AES128-SHA256 0xC0, 0x2F ECDHE RSA AES-GCM(128) SHA256 ECDHE-RSA-AES256-SHA384 0xC0, 0x30 ECDHE RSA AES-GCM(256) SHA384 The fields above are : {Tenable ciphertype} {Cipher ID code} Kex={key exchange} Auth={authentication} Encrypt={symmetric encryption method} MAC={message authentication code} {export flag}

TCP	443	www	✓ 1.00	Title: SSL Root Certification Authority Certificate Information Synopsis: A root Certification Authority certificate was found at the top of the certificate chain. Impact: The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain. See also : https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10) Resolution: Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies. Data Received: The following root Certification Authority certificate was found : -Subject : C=US/ST=New Jersey/L=Jersey City/O=The USERTRUST Network/CN=USERTrust RSA Certification Authority -Issuer : C=US/ST=New Jersey/L=Jersey City/O=The USERTRUST Network/CN=USERTrust RSA Certification Authority -Valid From : Feb 01 00:00:00 2010 GMT -Valid To : Jan 18 23:59:59 2038 GMT -Signature Algorithm : SHA-384 With RSA Encryption
-----	-----	-----	--------	--

TCP	443	www	✓ 1.00	Title: SSL Certificate Information Synopsis: This plugin displays the SSL certificate. Impact: This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate. Resolution: n/a Data Received: Subject Name: Common Name: *.cognillo.com Issuer Name: Country: GB State/Province: Greater Manchester Locality: Salford Organization: Sectigo Limited Common Name: Sectigo RSA Domain Validation Secure Server CA Serial Number: 4E C3 B7 79 1B CD 47 4B 6A 8B 4E AD E9 89 81 EF Version: 3 Signature Algorithm: SHA-256 With RSA Encryption Not Valid Before: Mar 27 00:00:00 2025 GMT Not Valid After: Apr 26 23:59:59 2026 GMT Public Key Info: Algorithm: RSA Encryption Key Length: 2048 bits Public Key: 00 EA 8D 3E 63 0C C6 C5 92 25 A6 EA 02 C1 B3 13 77 9E E3 8F F5 74 44 1D CA 28 7B 19 A7 73 61 1E 69 43 F0 AF 16 D9 42 93 0A A1 75 1B 27 01 6B 5A 59 87 F9 B9 76 C9 21 A0 F7 8F C2 A9 69 45 9E 9B 38 7C 08 D4 58 E4 18 28 57 20 16 25 FA 36 B9 15 13 4D 86 AD 16 BB 59 7D BE 91 17 F4 40 9E 66 53 0E 9D BF 6A 23 37 86 A0 60 BF ED C8 1E 39 29 BD 5E 40 C3 F1 FC 35 17 51 E7 83 C4 B3 83 48 A0 80 1B BE AF 88 06 8E AA 74 8E E4 0D D7 F3 EB 10 D9 BD A8 6D AC F3 3B DF 80 B0 00 7D AD BC 59 29 EC 9E A1 F4 74 86 34 3C 7A 84 03 05 28 E3 0D F4 59 FA E6 1E 77 96 82 9B E7 CD E4 B0 0C CC 7A 37 CC F0 D2 6F 5D 7E F7 15 1E 50 F4 22 B5 C6 E6 B0 52 B2 CE CE A5 6D 37 C2 B8 D3 60 F9 7B 7C 44 40 49 A5 29 A4 89 6C 28 76 93 46 20 09 3E 95 DF 48 4A 8F 25 97 A7 57 1E 54 4F 60 0C 12 52 BE 7B 92 DB D3 Exponent: 01 00 01 Signature Length: 256 bytes / 2048 bits Signature: 00 C7 5C 0C BB 07 34 70 48 9C 77 F3 69 8E 2E 33 64 99 C5 AB 2E 92 92 93 FE 9E EB 0D 6E FE 02 55 7A 96 2D 4D A9 69 21 A7 2E 7F AA D9 BF 40 C1 1A 97 C8 9B 73 A5 D7 B4 BC E1 91 8A 24 F2 FF 6E 71 B8 DA 83 78 95 1B F4 98 86 5A A1 33 E6 40 36 33 19 64 07 8F 4B ED 0B 6C EE 27 95 51 97 42 6D 91 BF EA BA 9F B4 7D 1E 04 50 C7 40 23 66 56 DB 59 9B DF 97 50 F3 71 5F 0B 88 55 CF B8 B0 3B A8 55 DC 9B 77 6E 51 A6 62 6C 46 77 F4 E2 B6 0A 78 3A BE 80 9F 39 2F 41 D9 AF 53 D5 D0 65 79 F2 3E DB 3B 6E 62 EB 51 39 BD AC A6 E9 13 2C 4B 2E 36 0A DA C9 FD 31 5B 7A 73 1D 04 A1 27 7D 58 3D DC AD 65 44 33 9C C8 91 46 80 56 B7 B5 40 7F C4 3E 95 42 11 8D BD 97 24 81 75 64 FF 27 B3 0D 9D F3 EA 57 5E 01 56 A6 E7 F0 C4 91 09 D9 41 4B B4 DF B6 F5 26 C8 3D 29 EC C0 8B 5A A5 2E 82 2F 09 FC 86 5E Extension: Authority Key Identifier(2.5.29.35) Critical: 0 Key Identifier: 8D 8C 5E C4 54 AD 8A E1 77 E9 9B F9 9B 05 E1 B8 01 8D 61 E1 Extension: Subject Key Identifier(2.5.29.14) Critical: 0 Subject Key Identifier: CD 14 20 0F 5B 88 C8 56 03 AD 56 D3 9F 3B 32 93 79 85 A3 1B Extension: Key Usage(2.5.29.15) Critical: 1 Key Usage: Digital Signature, Key Encipherment Extension: Basic Constraints(2.5.29.19) Critical: 1 Extension: Extended Key Usage(2.5.29.37) Critical: 0 Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1) Purpose#2: Web Client Authentication (1.3.6.1.5.5.7.3.2) Extension: Policies(2.5.29.32) Critical: 0 Policy ID #1:
-----	-----	-----	--------	---

1.3.6.1.4.1.6449.1.2.2.7 Qualifier ID #1: Certification Practice Statement(1.3.6.1.5.5.7.2.1) CPS URL: <https://sectigo.com/CPS> Policy ID #2: 2.23.140.1.2.1 Extension: Authority Information Access(1.3.6.1.5.5.7.1.1) Critical: 0 Method#1: Certificate Authority Issuers URI:
<http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt>
Method#2: Online Certificate Status Protocol URI: <http://ocsp.sectigo.com>
Extension: Subject Alternative Name(2.5.29.17) Critical: 0 DNS:
*.cognillo.com DNS: cognillo.com Extension: 1.3.6.1.4.1.11129.2.4.2
Critical: 0 Data: 04 82 01 67 01 65 00 75 00 96 97 64 BF 55 58 97 AD F7 43 87 68 37 08 42 77 E9 F0 3A D5 F6 A4 F3 36 6E 46 A4 3F 0F CAA9 C6 00 00 01 95 D6 EA 45 25 00 00 04 03 00 46 30 44 02 20 12 E8 4E 94 BF 6F 19 CB 9B F9 1B 29 1E 0A 9F 8F BD 40 B1 56 BE 38 35 47 FE AC 20 0A 8C 3F 29 87 02 20 0B 60 32 79 01 AD EC E8 45 4F 96 61 2D 7B D2 48 2A B3 A1 47 60 58 98 EF 05 F5 6C E5 05 E1 18 94 00 75 00 19 86 D4 C7 28 AA 6F FE BA 03 6F 78 2A 4D 01 91 AA CE 2D 72 31 0F AE CE 5D 70 41 2D 25 4C C7 D4 00 00 01 95 D6 EA 44 D9 00 00 04 03 00 46 30 44 02 20 20 8F 49 35 83 FF BD D8 5D 1C C4 C9 27 E9 D3 11 3F E6 2B 7D 2A 52 3A 3B BB AC DB E4 03 9D DC 8F 02 20 75 DD 3C 6E DE 26 DD 82 F6 F2 80 C0 72 52 8E 43 30 42 D3 DF B5 B3 A5 9F 81 8E C1 B6 08 CF AD E9 00 75 00 0E 57 94 BC F3 AE A9 3E 33 1B 2C 99 07 B3 F7 90 DF 9B C2 3D 71 32 25 DD 21 A9 25 AC 61 C5 4E 21 00 00 01 95 D6 EA 44 F0 00 00 04 03 00 46 30 44 02 20 59 63 75 2B AE B4 74 BD 65 D6 9E EF 25 1D F2 7D 07 BD FA F9 92 4A B1 78 50 B2 E5 B2 FC 30 D5 40 02 20 58 84 66 E7 2E 88 C9 78 2C 56 C5 8D B1 B8 4E F7 BE E4 DF D7 28 9A C8 4F D6 8B 30 AC CD 55 F4 57 Fingerprints : SHA-256
Fingerprint: 08 EF 77 1C 02 7D 54 75 01 10 38 D5 DD EF 16 33 A0 D5 03 26 67 65 16 D7 E6 A9 75 DA 4E 8D 18 62 SHA-1 Fingerprint: 82 5A 8F DD 53 6E 09 2F DC C5 9A 7C 33 EC 8F E8 11 FC F4 F3 MD5
Fingerprint: FF A2 42 DE 22 75 40 B3 13 63 E2 98 0A 5D 25 43 PEM
certificate : -----BEGIN CERTIFICATE-----
MIIGMDCCBRigAwIBAgIQTsO3eRvNR0tqi06t6YmB7zANBgkqhkiG9w0B
AQsFADCBjzELMAkGA1UEBhMCR0IxGzAZBgNVBAgTEkdyZWFOZXIgt
WfUy2hlc3RlcjEQMA4GA1UEBxMHU2FsZm9yZDEYMBYGA1UEChMP
U2VjdGlnbyBMaW1pdGVkMTcwNQYDVQQDEy5TZWN0aWdvIFJTSBE
b21haW4gVmFsaWRhdGlvbiBTZWN1cmUgU2VydmVyIENBMB4XDTI1M
DMYnZAwMDAwMFoXDTI2MDQyNjIzNTk1OVowGTEXMBUGA1UEAww
OKi5jb2duaWxsby5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwgg
EKAoIBAQDqjT5jDMbFkiWm6gLBsxN3nuOP9XREHcooexmnc2EeaUPwr
xbZQpMKoXUbjWFrWlmH+bl2ySGg94/CqWlFnps4fAjUWOQYKfCgFiX6
NrKVE02GrRa7WX2+kRf0QJ5mUw6dv2ojN4agYL/tyB45Kb1eQMPx/DUX
UeeDxLODSKCAG76viAaOqnSO5A3X8+sQ2b2obazzO9+AsAB9rbxZKey
eofR0hjQ8eoQDBSjjDfRZ+uYed5aCm+fn5LAMzHo3zPDSb11+9xUeUPQ
itcbmsFKyzs6lbTfCuNNg+Xt8REBJpSmkiWwodpNGIAK+ld9lSo8ll6dXHIR
PYAwSUR57ktvTAgMBAAGjggL7MIIC9zAfBgNVHSMEGDAWgBSNjF7EV
K2K4Xfpm/mbBeG4AY1h4TAdBgNVHQ4EFgQUzRQgD1ulyFYDrVbTnzs
yk3mFoxswDgYDVR0PAQH/BAQDAgWgMAwGA1UdEwEB/wQCMAAwH
QYDVR0IBBYwFAYIKwYBBQUHAWEGCCsGAQUFBwMCMekGA1UdIA
RCMEAwNAYLKwYBBAGyMQECAgcwJTAjBggrBgEFBQcCARYXaHR0c
HM6Ly9zZWNOaWdvLmNvbS9DUFMwCAYGZ4EMAQIBMIGEBggrBgEF
BQcBAQR4MHYwTwYIKwYBBQUHMAKGQ2h0dHA6Ly9jcnQuc2VjdGlnb
y5jb20vU2VjdGlnb1JTQURvbWVpblZhbGlkYXRpb25TZWN1cmVTZXJ2Z
XJDQS5jcnQwLwYIKwYBBQUHMAGGF2h0dHA6Ly9vY3NwLnNlY3RlY2
8uY29tMCCGA1UdEQQgMB6CDiouY29nbmlsbG8uY29tggxjb2duaWxsby
5jb20wggF7BgorBgEEAdZ5AgQCBIIBawSCAWcBZQB1AJaXZL9VWJet9
0OHaDclQnfp8DrV9qTzNm5GpD8PyqnGAAABldbqRSUAAAQDAEYwRA
IgeuhOIL9vGcub+RspHggfj71AsVa+ODVH/qwgCow/KYcCIAtgMnkBrezo
RU+WYS170kgqs6FHYFiY7wX1bOUF4RiUAHUAGYbUxyiqb/66A294Kk0
BkarOLXlxD67OXXBBLsVMx9QAAAGV1upE2QAABAMARjBEAiAgj0k1g

				/+92F0cxMkn6dMRP+YrfSpSOju7rNvkA53cjwlgdd08bt4m3YL28oDAclKO QzBC09+1s6WfgY7BtgjPrekAdQAOV5S8866pPjMbLJkHs/eQ35vCPXEyJ d0hqSWsYcVOIQAAAZXW6kTwAAAEAwBGMEQCIFldSuutHS9Zdae7y Ud8n0Hvfr5kkqxeFCy5bL8MNVAAiBYhGbnLojJeCxWxY2xuE73vuTf1yiaY E/WizCszVX0VzANBqkqhkiG9w0BAQsFAAOCAQEAX1wMuwc0cEicd/Npj i4zZJnFqy6SqpP+nusNbv4CVXqWLU2paSGnLn+q2b9AwRqXyJtzpde0v OGRiiTy/25xuNqDeJUb9JiGWqEz5kA2MxlkBA9L7Qts7ieVUZdCbZG/6rqft H0eBFDHQCnmVttZm9+XUPNxXwulVc+4sDuoVdybd25RpmJsRnf04rYK eDq+gJ85L0HZr1PV0GV58j7bO25i61E5vaym6RMSSy42CtrJ/TFbenMdB KEnfVg93K1IRD0cyJFGgFa3tUB/xD6VQhGNvZckgXVvk/yezDZ3z6ldeAVa m5/DEkQnZQUu037b1Jsg9KezAi1qLLolvCfyGXg== -----END CERTIFICATE-----
TCP	443	www	✓ 1.00	Title: TLS Supported Groups Synopsis: The remote service negotiates TLS supported curve groups. Impact: This plugin detects which TLS supported groups entries are supported by the remote service. Resolution: n/a Data Received: These are the TLS supported groups offered by the remote server : TLS supported groups : Name Code ----- x25519 0x001d secp256r1 0x0017 x448 0x001e secp521r1 0x0019 secp384r1 0x0018 ffdhe2048 0x0100 ffdhe3072 0x0101 ffdhe4096 0x0102 ffdhe6144 0x0103 ffdhe8192 0x0104
TCP	443	www	✓ 1.00	Title: SSL / TLS Versions Supported Synopsis: The remote service encrypts communications. Impact: This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications. Resolution: n/a Data Received: This port supports TLSv1.3/TLSv1.2.

TCP	443	www	✓ 1.00	Title: Apache HTTP Server Version Synopsis: It is possible to obtain the version number of the remote Apache HTTP server. Impact: The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner. See also : https://httpd.apache.org/ Resolution: n/a Data Received: URL : https://cognillo.com/ Version : unknown Source : Server: Apache backported : 0
TCP	80	www	✓ 1.00	Title: Apache HTTP Server Version Synopsis: It is possible to obtain the version number of the remote Apache HTTP server. Impact: The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner. See also : https://httpd.apache.org/ Resolution: n/a Data Received: URL : http://cognillo.com/ Version : unknown Source : Server: Apache backported : 0

TCP	443	www	✓ 1.00	Title: Smartbedded Meteobridge Web Detection Synopsis: The web UI for Smartbedded Meteobridge was detected on the remote host. Impact: Smartbedded Meteobridge, a dedicated weather monitoring application, is running on the remote host. Note: Basic HTTP Authentication credentials are required to obtain the version. See also : https://www.meteobridge.com/wiki/index.php?title=Meteobridge_VM http://www.nessus.org/u?5ceb65be Resolution: n/a Data Received: URL : https://cognillo.com/cgi-bin/meteobridge Version : unknown Authenticated : False
TCP	80	www	✓ 1.00	Title: Smartbedded Meteobridge Web Detection Synopsis: The web UI for Smartbedded Meteobridge was detected on the remote host. Impact: Smartbedded Meteobridge, a dedicated weather monitoring application, is running on the remote host. Note: Basic HTTP Authentication credentials are required to obtain the version. See also : https://www.meteobridge.com/wiki/index.php?title=Meteobridge_VM http://www.nessus.org/u?5ceb65be Resolution: n/a Data Received: URL : http://cognillo.com/cgi-bin/meteobridge Version : unknown Authenticated : False

TCP	443	www	✓ 1.00	Title: Strict Transport Security (STS) Detection Synopsis: The remote web server implements Strict Transport Security. Impact: The remote web server implements Strict Transport Security (STS). The goal of STS is to make sure that a user does not accidentally downgrade the security of his or her browser. All unencrypted HTTP connections are redirected to HTTPS. The browser is expected to treat all cookies as 'secure' and to close the connection in the event of potentially insecure situations. See also : http://www.nessus.org/u?2fb3aca6 Resolution: n/a Data Received: The STS header line is : Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
TCP	443	www	✓ 1.00	Title: Web Server No 404 Error Code Check Synopsis: The remote web server does not return 404 error codes. Impact: The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page. SecurityMetrics has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate. Resolution: n/a Data Received: CGI scanning will be disabled for this host because the host responds to requests for non-existent URLs with HTTP code 301 rather than 404. The requested URL was : https://cognillo.com/HGglQIR7p1_.html

TCP	80	www	✓ 1.00	Title: Web Server No 404 Error Code Check Synopsis: The remote web server does not return 404 error codes. Impact: The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page. SecurityMetrics has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate. Resolution: n/a Data Received: CGI scanning will be disabled for this host because the host responds to requests for non-existent URLs with HTTP code 301 rather than 404. The requested URL was : http://cognillo.com/HGglQIR7p1_.html
-----	----	-----	--------	---